An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT

Jianying Qiu

Kai Fan

Kuan Zhang

Qiang Pan

Hui Li

See next page for additional authors

Authors

Jianying Qiu, Kai Fan, Kuan Zhang, Qiang Pan, Hui Li, and Yintang Yang

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 5, 2019, accepted December 1, 2019, date of publication December 6, 2019,
date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2958089

An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT

JIANYING QIU[1], KAI FAN[1], (Member, IEEE), KUAN ZHANG[2], (Member, IEEE), QIANG PAN[1], HUI LI[1], (Member, IEEE), AND YINTANG YANG[3], (Member, IEEE)

[1]State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China
[2]Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, Lincoln, NE 68588, USA
[3]Key Laboratory of the Ministry of Education for Wide Band-Gap Semiconductor Materials and Devices, Xidian University, Xi'an 710071, China

Corresponding author: Kai Fan (kfan@mail.xidian.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802600, in part by the National Natural Science Foundation of China under Grant 61772403 and Grant U1836203, in part by the Natural Science Foundation of Shaanxi Province under Grant 2019ZDLGY12-02, in part by the Shaanxi Innovation Team Project under Grant 2018TD-007, in part by the Xi'an Science and Technology Innovation Plan under Grant 201809168CX9JC10, and in part by the National 111 Program of China under Grant B16037.

ABSTRACT The Internet of Things (IoT) is developing towards smart and mobile Internet of Things (SM-IoT), which has made great progress. Due to the inherent heterogeneity, distribution, intensive communication, and resource constraints of SM-IoT, efficient security and privacy communication protocols become a particularly critical challenge. Signcryption has received considerable attention. Various signcryption schemes have been proposed to solve secure communication. However, most of them are low in efficiency, without the consideration of characteristics of the SM-IoT. In this paper, we propose a signcryption scheme to achieve efficient secure multi-message and multi-receiver communication for the heterogeneous and distributed SM-IoT. We develop Identity-based Cryptography (IBC) and Certificateless Cryptography (CLC) to solve the certificate management problem. Our scheme no longer needs wireless secure channel during key generation phase of traditional CLC system, which improves the applicability of our scheme in wireless SM-IoT environment. There is no expensive operations, such as bilinear pairing, in our scheme. In addition, our scheme outsources part of the verification overhead from the SM-IoT users to the gateway without revealing user privacy. The performance evaluation shows that the computation efficiency in both sender and receiver side is improved in our scheme.

INDEX TERMS Certificateless cryptography (CLC), identity-based cryptography (IBC), heterogeneous, verification outsourcing, smart mobile Internet of Things (SM-IoT), multi-massage and multi-receiver signcryption.

I. INTRODUCTION

The Internet of Things (IoT) is emerging as an important part of the new generation of information technology [1]. The IoT aims to create an open global network connecting people, things and data, providing a ubiquitous interconnected mobile and smart sensor network for smart cities [2]. Security and privacy are always the crucial issues of IoT.

In order to protect the security and privacy of the IoT environment, extensive research on physical layer security [3], authentication (such as RFID authentication [4]–[6]), secure access control mechanism (e.g., access control scheme based on attribute base encryption [7]), secure communication, network traffic and data analysis method [8]–[10], and threat detection technology [11], [12] has been carried out.

The IoT architecture consists of four layers: sensing layer, interconnection layer, data layer and service layer [13]. The purpose of the service layer or the application layer is to provide various typical/personalized services or customized recommendations for users. IoT is developing towards the Smart and Mobile Internet of Things (SM-IoT) [14], and has made great progress. For example, smart traffic management

The associate editor coordinating the review of this manuscript and approving it for publication was Zheli Liu.

systems enable cities aims to control traffic facilities and improve the efficiency. Smart medical systems can collect patients' data and help medical professionals to monitor the physical condition of patients in real time. At present, the demand for services based on SM-IoT is increasing and tending to diversify, such as medical services, weather forecasting, various resource management, environmental awareness and data acquisition. Because of the flattening of services, each authentication entity in SM-IoT can be a service sender. It makes the information and decentralized communication technology system face more and more network security threats [12], since many services are related to users' sensitive information and private data.

In addition, it is noticeable that the number of IoT devices is growing dramatically. Cisco predicted that, by 2025, 500 billions devices will connect the Internet [15]. The SM-IoT allows them to interact with each other [16]. It indicates that there will be more intensive communication between people and things, things and things. The IoT system is usually deployed in a distributed environment. In a distributed environment, IoT entities exchange information dynamically to provide a decentralized and scalable infrastructure, to support billions of devices generating and exchanging large amount of data. Decentralized communication has become a crucial trend of SM-IoT, such as the researches on block-chain based mechanism [17] and device-to-device (D2D) communication technology. Meanwhile, we need more efficient secure schemes and mechanisms that can fulfill the heterogeneity and distribution of the SM-IoT environment. Among numerous cryptography methods, signcryption, a cryptography primitive can be applied to decentralized communication environment, has received considerable attention because of its high efficiency and security. Various efficient signcryption schemes have been proposed to achieve secure decentralized communication.

In this article, we consider the requirements to provide efficient personalized services for SM-IoT users, while ensuring security and privacy.

General multi-cast mechanism can only provide typical services through centralized approach, but can not provide personalized services for each user. Lacking of encryption and authentication mechanism makes SM-IoT devices more vulnerable to malicious attacks and threats. Multi-message and multi-receiver signcryption is an effective method to solve the problem. Multi-message and multi-receiver signcryption can complete the encryption and signature process of different messages sent to different receivers in one logical step. Receivers get customized messages that belongs to themselves, while other receivers can not decrypt them. It ensures both data privacy and communication security. At the same time, this method does not increase the cost of the SM-IoT receiver.

The challenging issues motivate us to design a scheme to complete secure communications from service sender of IBC system to the receivers of CLC system, which meets the needs of personalized multi-cast in the SM-IoT.

TABLE 1. Notations.

Symbol	Definition
ECC	Elliptic Curve Cryptography.
G	The addition cyclic group of points on ECC.
p	Large Integer prime.
P	Generator of G.
IBC	Identity-based Cryptography.
CLC	Certificateless Cryptography.
PKG	Private Key Generator.
KGC	Key Generate Center.
Z_p^*	Non-zero multiplicative group with large prime p.
s_1, s_2	The master key of the PKG or the KGC.
H_i	Hash functions.
PK_i	Public key of user with ID_i.
SK_i	Private key of user with ID_i.
Enc_ρ	Symmetric encryption algorithm with symmetric key ρ.
Dec_ρ	Symmetric decryption algorithm.
Pr	The probability of an event.

In this paper, we propose a multi-message and multi-receiver signcryption scheme for SM-IoT system, which can provide data privacy and communication security with higher efficiency. Our contributions can be summarized as follow:

1) We propose an efficient multi-message and multi-receiver signcryption scheme, which is constructed based on ECC, employing scalar point multiplication operations rather than bilinear pairing. The calculation complexity of the scheme is relatively lower.
2) Our scheme is a heterogeneous communication scheme from the sender of IBC to receivers of CLC. It explores the PKG and the KGC to generate keys for users of IBC and CLC systems respectively. It is more practical in SM-IoT applications.
3) In order to reduce the SM-IoT receivers' computing overhead, we outsource part of the receivers' verification computation operations to the gateway, and verify the computation. Meanwhile, the gateway can not access the privacy information of the SM-IoT receivers.
4) Our scheme hides the partial private key for wireless network users of CLC system during the key generation process. A secure channel is no longer needed between the SM-IoT user and the KGC, which increases the security of the scheme.

The structure of this paper is as follows: Section 2 reviews the related works. The security assumptions, network model, system model, and security model are described at Section 3 in detail, while Section 4 presents the proposed scheme. Correctness proof and security analysis of the proposed scheme are demonstrated in section 5. In section 6, we compare the function and performance between the proposed scheme and previous ones, and simulate the execution time of several schemes. A summary of this paper is made in Section 7.

In order to make the article easier to understand, TABLE 1 displays the abbreviations and notations used in this paper.

II. RELATED WORKS

In 1997, Zheng [18] fitst proposed the primitive of signcryption, which can complete signature and encryption in one

single logical step. Initially, the schemes proposed by the researchers were based on public key infrastructure (PKI), e.g., schemes [19], [20]. But PKI has the burden of certificate management, which requires both storage and time. Considering the certificate management burden, as early as 1984, Shamir [21] introduced the concept of identity-based cryptography (IBC) to solve this problem. In IBC system, the user's public key is calculated based on his/her identity information. Thus, IBC gets rid of the burden of certificate management.

In 2002, Malone-Lee [22] combined IBC and signcryption, and proposed identity-based signcryption (IBSC) scheme. Libert and Quisquater [23] proposed three IBSC schemes after pointing out the insecurity of Malone-Lee's scheme. In 2003, Chow *et al.* [24] proposed a IBSC scheme which can provide both public verifiability and forward security. And Boyen [25] proposed a IBSC scheme with public verifiability, forward security, and anonymity. Li and Khan [26] made a survey, and summarized the future research trend of IBSC, including designing and constructing new and efficient IBSC schemes with special properties in the standard model, constructing postquantum signcryption, and finding new applications for IBSC. IBSC has great advantage in computation and communication overhead, researchers have applied it to the Internet of Things. In 2017, Karati *et al.* [27] presented an IBSC scheme for Industrial Internet of Things (IIoT) environment. However, the IBSC has the problem of excessive dependence on PKG, which is inherent in identity-based encryption system, because it needs the PKG to generate the user's full private key. Once the PKG is attacked, the system security will be greatly effected or even be destroyed.

In 2003, Al-Riyami and Peterson [28] proposed the concept of certificateless public key cryptography (CL-PKC), which changes the way the user's public and private keys were generated. The user generates a secret value, and combines it with the partial private key generated by the KGC to obtain full private key. Therefore, the key escrow problem is addressed by CL-PKC. In 2008, Barbosa and Farshim [29] researched the Certificateless Signcryption System (CLSC) and proposed the first certificateless signcryption scheme. However, their scheme requires six pairing operations during signcrypt and designcrypt phase which is low in efficiency. Wu and Chen [30] proposed a new CLSC scheme which needs four pairing operations, and Sharmila *et al.* [31] analyzed that their scheme was insecure. Then, in 2010, Liu *et al.* [32] proposed a novel scheme which is secure in the standard model, but their scheme needs five pairing operations. Xie and Zhang [33] proposed a new certificateless scheme which only needs two pairings. Thus, their scheme is more efficient than other CLSC schemes proposed before. However, all of these schemes employed bilinear pairing operations, whose efficiency is much lower than that of scalar multiplication over the elliptic curve group. In 2009, Sharmila *et al.* [34] proposed the first CLSC scheme without bilinear pairing and prove it in the random oracle model. Henceforth, Certificateless signcryption tends to be more lightweight. In 2010, Xie and Zhang [35] proposed a pairing-free CLSC scheme, which is more efficient than all previous constructions. Since then, many CLSC schemes without bilinear pairing have been proposed (e.g., [36]–[38]). Researchers put forward many CLSC schemes combined with the different mechanisms and other technologies, which are suitable for various environments. In 2017, Li *et al.* [39] proposed a certificateless signcryption scheme which achieves the public verifiability, ciphertext authenticity as well as insider security. And they designed an access control scheme based on the proposed certificateless signcryption scheme. References [38] and [40] combine the characteristics of the IoT environment, improve the efficiency of CLSC signcryption, and make it suitable for the application of IoT safely and effectively.

Furthermore, the schemes above are constructed for one-to-one communication, which is unable to meet the growing demand for multicast communication. There are schemes provide the sender with the function that send one message to different receivers. In 2006, the first multi-receiver signcryption scheme based on IBC was proposed by Duan and Cao [41]. Schemes [42], [43] are constructed based on identity-based signcryption, which ensure the anonymity of receivers. Hung *et al.* [44], Islam *et al.* [45], and Pang *et al.* [46] proposed multi-receiver certificateless signcryption schemes respectively.

In the SM-IoT environment we consider, there are demands of sending personalized services and customized messages, which means we need to send different messages to different receivers at a time. The SM-IoT has raised the requirement for secure multi-message and multi-receiver communication services. The concept of multi-receiver and multi-message signcryption was first proposed by Seo and Kim [47] in 1999. They construct a multi-message and multi-receiver domain authentication signcryption scheme. Users in the authentication domain can verify the validity of the message and decrypt it to get their own. Elkamchouchi and Hagras [48] proposed a multi-message and multi-receiver signcryption scheme based on ECC which reduced the computational overhead. Kumar and Ansari [49] proposed a scheme which supports public verifiability in 2013. But it is regretful that their scheme uses time-consuming modular exponentiation operations. And in 2019, Pang *et al.* [50] constructed a certificateless signcryption scheme based on ECC, which is efficient and ensures the anonymity of receivers. However, because of the complexity of communication environment, different communication terminals may be in different security cryptography environment, which means that we need to consider signcryption schemes for heterogeneous systems. This situation is more common in the SM-IoT environment. In order to adapt to the heterogeneity of the SM-IoT, heterogeneous signcryption schemes have received great attention. In 2010, Sun and Li [51] proposed the multi-receiver signcryption scheme for secure communication between IBC and PKI. Huang *et al.* [52] proposed a heterogeneous scheme that allows the sender in the IBC system to send a message to the

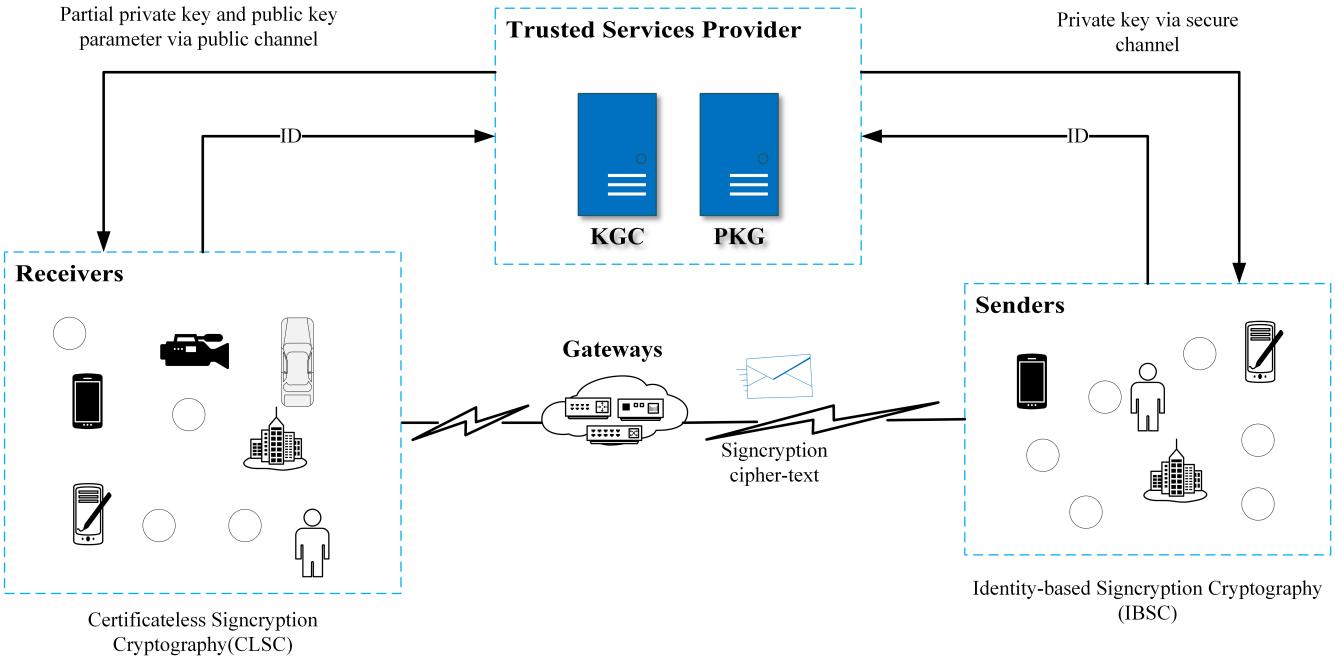

FIGURE 1. Network model.

receiver in the PKI system, and scheme [53] was constructed based on CLC and PKI. Obviously, these schemes generally have the problem of certificate management overhead, because they are constructed based on PKI. Li *et al.* [54] and Niu *et al.* [55] proposed a multi-receiver signcryption scheme between IBC and CLC respectively, but their schemes employ bilinear pairing operation, which makes their scheme low inefficient.

III. PRELIMINARIES

In this section, we briefly review the definition of security assumption, and then give the network model, general model and security model of the scheme.

A. SECURITY ASSUMPTIONS

Assuming p is a large integer prime, and G is an addition cyclic group of points on ECC with order p, P is a generator of G, Z_p^* is a nonzero multiplicative group based on p. We define the Elliptic Curve Discrete Logarithm Problem (ECDLP) and Computational Diffie-Hellman Problem (CDHP) as follow:

1) ECDLP

Given two elements $P, Q \in G$, and $Q = aP$, where $a \in Z_p^*$, computing a is called ECDLP.

Definition 1: The probability advantage of extracting ECDLP by any probability polynomial time (PPT) adversary A defined as follow is negligible.

$$Adv_A^{ECDLP}(k) = \Pr[A(P, aP) = a | a \in Z_p^*] \quad (1)$$

2) CDHP

Given tuple (P, aP, bP), where $a, b \in Z_p^*$, computing abP is called CDHP.

Definition 2: The probability advantage of extracting CDHP by any PPT adversary A defined as follow is negligible.

$$Adv_A^{CDHP}(k) = \Pr[A(P, aP, bP) = abP | a, b \in Z_p^*]. \quad (2)$$

B. NETWORK MODEL

As shown in Fig. 1, our network model contains four entities, the Trusted Service Provider, including the KGC for CLC and the PKG for IBC, Resource Senders of IBC system, receivers of CLC system and the gateway. We assume the PKG and KGC are fully trusted, and the gateway is honest but curious, which means that the gateway honestly follows the scheme, but is curious to decrypt the ciphertext. The sender needs to be authorized by the PKG. The PKG generates a private key for the sender of the IBC system, and the KGC generates partial private keys for receivers of the CLC system. Then, the sender signcrypts messages and transmits the signcryption ciphertext to the gateway. The gateway computes the signcryption verification parameter, and transfers it with ciphertext to receivers. Only the designated receivers can correctly verify the parameter and signature, and then decrypt the corresponding signcryption ciphertext. This model supplies an efficient and secure one-to-many decentralized communication for heterogeneous SM-IoT.

C. GENERAL MODEL

The general model of our scheme is composed of four main algorithms [39], [55], *Setup Algorithm, Key Extraction Algorithm, Signcryption Algorithm, Designcryption Algorithm*, described as follow.

1) SETUP ALGORITHM

With security parameter λ as input, the PKG runs the *PKG setup algorithm* and KGC runs the *KGC setup algorithm* to generate their master keys and system public keys, and keep master key secret respectively. Then, the Trusted Service Provider publishes the public parameter *param*.

2) KEY EXTRACTION ALGORITHM

This algorithm is divided into *Identity-Based Cryptography Key Generation(IBC-KG) algorithm* and *Certificateless Cryptography Key Generation(CLC-KG) algorithm* as follow:

IBC-KG. This algorithm runs by PKG of the IBC system. The sender sends his identity ID_s to the PKG. The PKG generates corresponding private key SK_s for the sender and returns back through secure channel.

CLC-KG. The algorithm runs by KGC and users of the CLC system.

1) *Set Secret Value Algorithm:* The receiver of CLC system runs this algorithm to generate a secret value x_i, which is used to construct his full private key and the corresponding public key parameter X_i.
2) *Extract Partial Private Key Algorithm:* The algorithm runs by the KGC of CLC system. With ID_i and X_i as inputs, the KGC generates corresponding partial private key d_i hiding in u_i, and public key parameter T_i, then transmits (u_i, T_i) through public channel.
3) *Set Public Key Algorithm:* The algorithm runs by the receiver. With T_i and public key parameter X_i as inputs, user generates his public key PK_i. Then, the user sends PK_i to the KGC for publication.
4) *Set Full Private Key Algorithm:* The algorithm runs by the receiver. After obtaining partial private key d_i from u_i, with secret value x_i as input, the user generates his/her full private key SK_i.

3) SIGNCRYPTION ALGORITHM

This algorithm runs by the sender of IBC system. Taken sender's private key SK_s and system public parameter *param*, a set of receivers' PK_i and the messages $M = \{m_i | i = 1, 2, \ldots, n\}$ as inputs, the algorithm returns the full signcryption ciphertext σ.

4) DESIGNCRYPTION ALGORITHM

With ciphertext σ, the gateway computes the signcryption verification parameter and transmits to receivers. With the public key of sender and the private key of receiver SK_i as inputs, the receiver verifies the parameter, and then runs Designcryption algorithm to verify and recover his plaintext message m_i.

D. SECURITY MODELS

This subsection defines the security model [46], [56], [57] of the proposed scheme under random oracal. The confidentiality of the proposed scheme is defined based on the concept of indistinguishable against adaptive chosen ciphertext attacks (IND-CCA2), considering two types of adversary. A Type I adversary A_I is a dishonest user, who can not know the master key of KGC but has the right to replace any user's public key. A Type II adversary A_{II} is a curious but honest KGC, who knows the master key but does not have the authorize to replace user's public key. The authorization is defined based on the concept of existential unforgeability against adaptive chosen message attacks (EUF-CMA).

1) GAME 1: CONFIDENTIALITY WITH ADVERSARY A_I

Game 1 is defined to meet IND-CCA2 against A_I. The game is an interaction between the challenger C and the adversary A_I under IND-CCA2. Π is an IBC-CLC multi-message and multi-receiver signcryption algorithm. The game is shown as follows.

Setup: Given security parameter λ, challenger C runs the *Setup Algorithm*, generates system public parameter *param*, sends to adversary A_I, but keeps KGC's master key s_2 secret. And A_I chooses a set of target identities $I = \{ID_i | i = 1, 2, \ldots, n\}$.

Phase 1: A_1 makes polynomial bounded number of queries to C.

1) *Partial private key query:* A_I chooses an $ID_j \notin I$ and sends to C. C runs the *Extract Partial Private Key Algorithm* to generate corresponding partial private key and then sends it back to A_I.
2) *Secret value query:* A_I sends ID_j to the challenger C. C runs the *CLC-KG Algorithm* to get secret value of user.
3) *Public key query:* A_I queries for the public key of ID_j, and C runs *Set Public Key Algorithm* and returns the result to the adversary.
4) *Replace public key:* The adversary may replace the public key of any user.
5) *Signcryption query:* With the public key sender ID_s, receivers $I^* = \{ID_j | j = 1, 2, \ldots, n, j \neq i\}$, the adversary A_I queries for signcryption of message set $M = \{m_1, m_2, \ldots, m_n\}$. The challenger C runs the *Signcryption Algorithm* to generate corresponding signcryption ciphertext σ and returns it back to A_I.
6) *Designcryption query:* The adversary A_I submits a signcryption ciphertext σ under sender ID_s, receivers $I^* = \{ID_j | j = 1, 2, \ldots, n, j \neq i\}$. C runs the *Designcryption Algorithm* to compute the result and then sends back to A_I.

Challenge: A_I chooses two plaintext M_0, M_1, and ID_s, $ID_i \in I$, A_I is not allowed to query the partial private key of ID_i in *Phase 1*. Then, C selects $\beta \in 0, 1$, and runs the

Signcryption Algorithm and generates corresponding ciphertext $\sigma*$ to send back to A_I.

Phase 2: A_I can query as Phase 1, but can not query partial private key of any receiver whose $ID_i \in I$, or private key of receivers whose public key has been replaced, and not query for the designcryption of $\sigma*$.

Guess: A_I produces a bit β'. If $\beta' = \beta$, then A_I wins the game. The advantage of A_I is defined as follow:

$$Adv_{\Pi}^{IND-CCA\ 2}(A_I) = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right| \tag{3}$$

Definition 3: If the probability advantage of A_I to win *Game 1* meets that $Adv_{\Pi}^{IND-CCA\ 2}(A_I) \leq \varepsilon$ within PPT τ, where ε is the non-negligible advantage. Then we said algorithm Π is IND-CCA2-I secure.

2) GAME 2: CONFIDENTIALITY WITH ADVERSARY A_{II}

Game 2 is defined to meet IND-CCA2 against A_{II}. The game is an interaction between the challenger C and the adversary A_{II} under IND-CCA2. Π is an IBC-CLC multi-message and multi-receiver signcryption algorithm. The game is shown as follows.

Setup: Given security parameter λ, challenger C setup as in *Game 1*, but sends *param*, and master keys s_1, s_2 to adversary A_{II}. The adversary A_{II} chooses a set of target receivers $I = \{ID_i | i = 1, 2, \ldots, n\}$.

Phase 1: The adversary A_{II} can make polynomial bounded number of queries as in *Phase 1* of *Game 1*. The challenger C makes corresponding responds.

Challenge: A_{II} chooses two plaintext M_0, M_1, and ID_s, $ID_i \in I$, then submits to C. A_{II} is not allowed to make *Secret Key query* of $ID_i \in I$ in Phase 1. The challenger runs *Signcryption Algorithm* to generate corresponding ciphertext σ^*, and returns to A_{II}.

Phase 2: A_{II} performs the queries as in *Phase 1*, except *Secret value query* of $ID_i \in I$, *private key query* of receivers whose public key has been replaced, and *Designcryption query* of σ^*.

Guess: The adversary A_{II} produces a bit β'. If $\beta' = \beta$, A_{II} wins the game. And the advantage of A_{II} is defined as follow:

$$Adv_{\Pi}^{IND-CCA\ 2}(A_{II}) = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right| \tag{4}$$

Definition 4: If the probability advantage of A_{II} to win *Game 2* meets that $Adv_{\Pi}^{IND-CCA\ 2}(A_{II}) \leq \varepsilon$ within PPT τ, where ε is the non-negligible advantage. Then we say the algorithm Π is IND-CCA2-II secure.

3) GAME 3: UNFORGEABILITY

Game 3 is defined to meet EUF-CMA against the forger F. The game is an interaction between the challenger C and the forger F under EUF-CMA. Π is a IBC-CLC multi-message and multi-receiver signcryption algorithm. The game is shown as follows.

Setup: Given security parameter λ, challenger C runs the *Setup Algorithm* to generate public parameter *param*, and master keys. Then sends the *param* to the forger F, and keeps master key of PKG secret. F chooses a target identity ID'_s.

Attack: F makes polynomial queries as follows.

1) *Private key query:* F submits an $ID_s \neq ID'_s$ to challenger C. C runs the *IBC_KG Algorithm* to generate corresponding private key of ID_s and returns it back to F.
2) *Signcryption query:* F submits ID_s, $ID_i (i = 1, 2, \ldots, n)$, and message M. C runs the *Signcryption Algorithm* to generate corresponding ciphertext σ and return it back to F.

Forgery: F produces a σ' with sender's identity ID'_s, whose private key SK'_s has never been queried. F wins if the Designcryption do not return a $\perp$.

Definition 5: An algorithm is EUF-CMA secure, if there is no PPT adversary which can win *Game 3* with non-negligible advantage.

IV. PROPOSED SCHEME

This section illustrates our signcryption scheme in detail. The proposed scheme involves four participants: KGC, PKG, sender ID_s, and n authorized receivers with identities $ID_1, ID_2, \ldots, ID_n$. The four algorithms described as follow:

A. SETUP ALGORITHM

With a security parameter λ as input, system randomly selects a prime p ($q \geq p^k$, k is a long integer.), and generates an ecliptic curve E defined on finite filed F_p. Then, chooses an additive group G on E and its generator P with order p. Because of the heterogeneity of SM-IoT environment, we use the PKG and the KGC to generate keys for users in different cryptography systems respectively.

1) PKG SETUP

Randomly chooses an integer $s_1 \in Z_p^*$ where s_1 is the master key that only PKG knows, and one hash function: $H_0 : \{0, 1\}^* \times G \times G \rightarrow Z_p^*$. Then, computes $P_1 = s_1 P$, and P_1 is the public key of PKG.

2) KGC SETUP

Randomly chooses an integer $s_2 \in Z_p^*$ as the master key, and computes $P_2 = s_2 P$ as KGC's public key. Then, defines five hash functions as follow:

$$\begin{aligned}
&H_1 : \{0, 1\}^* \times G \times G \rightarrow Z_p^*,\\
&H_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \times G \rightarrow Z_p^*,\\
&H_3 : Z_p^* \rightarrow \{0, 1\}^*,\\
&H_4 : Z_p^* \times G \rightarrow \{0, 1\}^*,\\
&H_5 : \{0, 1\}^* \times G \times G \times \{0, 1\}^* \times Z_p^* \times Z_p^* \times \ldots \times Z_p^*\\
&\qquad \rightarrow Z_p^*.
\end{aligned}$$

Chooses symmetric encryption/decryption function as Enc_ρ / Dec_ρ. ρ is a symmetric key.

Then, publishes the system's public parameter $param = \langle E, G, p, P, P_1, P_2, H_0, H_1, H_2, H_3, H_4, H_5, Enc_\rho, Dec_\rho \rangle$, and keep master keys s_1, s_2 secret respectively.

B. KEY EXTRACTION ALGORITHM

This algorithm is divided into *IBC-KG Algorithm* and *CLC-KG Algorithm* for the sender and the receivers respectively.

1) IBC-KG ALGORITHM

Sender transmits his ID_s to PKG. PKG randomly selects an integer $t_s \in Z_p^*$, computes $T_s = t_s P$, and $d_s = t_s + s_1 h_s (\text{mod } p)$, where $h_s = H_0(ID_s, T_s, P_1)$. Finally, returns $SK_s = (T_s, d_s)$ back via secure channel.

2) CLC-KG ALGORITHM

Receivers of CLC system obtain their partial private keys, generate their full private keys and public keys as follow:

Set Secret Value Algorithm: Receiver R_i with identity ID_i randomly selects an integer $x_i \in Z_p^*$, and computes $X_i = x_i P$, then sends (ID_i, X_i) to the KGC.

Set Partial Private Key Algorithm: Upon receiving ID_i and X_i, KGC randomly chooses an integer $t_i \in Z_p^*$, compute $T_i = t_i P$, and $d_i = t_i + s_2 h_i (\text{mod } p)$, where $h_i = H_1(ID_i, T_i, P_2)$. Then, compute $u_i = d_i + H_1(ID_i, s_2 X_i, T_i)$, KGC transmits T_i and u_i through public channel.

Set Public Key Algorithm: Upon receiving T_i and u_i from KGC, the receiver checks the equation:

$$u_i P = T_i + h_i P_2 + H_1(ID_i, x_i P_2, T_i) P \tag{5}$$

if the equation holds, the receiver accepts T_i and u_i, and sets $PK_i = h_i^{-1}(T_i + X_i)$ as his public key, and sends PK_i to KGC for publication. Otherwise, the receiver rejects T_i and u_i.

Set Full Private Key Algorithm: The receiver of the SM-IoT environment obtain

$$d_i = u_i - H_1(ID_i, x_i P_2, T_i) \tag{6}$$

Then, sets $SK_i = (x_i, d_i)$ as his full private key.

C. SIGNCRYPTION ALGORITHM

With the private key SK_s of sender, the public parameter $param$, the receiver's identity ID_i and public key PK_i $(i = 1, 2, \ldots, n)$ as input, the sender in IBC system runs the algorithm as follow:

1) Randomly chooses two integers $r_1, r_2 \in Z_p^*$, and computes $R_1 = r_1 P, R_2 = r_2 P$.
2) Computes $U_i = r_1 h_i (PK_i + P_2)$ and $\gamma_i = H_2(ID_s, ID_i, U_i, R_1)$, for each receiver.
3) Computes $c_i = m_i \oplus H_3(\gamma_i)$, and constructs $C = \{H_4(\gamma_1, R_1)||c_1, \gamma_2, R_1)||c_2, \ldots, H_4(\gamma_n, R_1)||c_n\}$.
4) Randomly chooses $\theta \in Z_p^*$. Then, computes

$$\begin{aligned} f(x) &= \prod_{i=1}^{n} (x - \gamma_i) + \theta (\text{mod} p) \\ &= x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \end{aligned} \tag{7}$$

$a_i \in Z_p^*$, and sets $A = \{a_i | i = 0, \ldots, n-1\}$.

5) Computes $h = H_5(ID_s, R_1, R_2, C, \theta, a_0, \ldots, a_{n-1})$, $\rho = H_3(\theta)$ and $S = Enc_{(\rho)}(C)$.
6) Computes $\nu = (hr_2 + d_s)^{-1} r_1 (\text{mod} p)$.

Finally, the sender sets $\sigma = (S, R_2, \nu, h, A)$ as signcryption ciphertext and broadcasts it to the SM-IoT receivers of CLC system through communication channel.

D. DESIGNCRYPTION ALGORITHM

Given $\sigma = (S, R_2, \nu, h, A)$, and receiver's private key, *Designcryption Algorithm* runs as follow:

First, the gateway obtain the sender's key T_s and performs as follow.

1) Computes

$$R_1' = \nu(hR_2 + T_s + h_s P_1) \tag{8}$$

where $h_s = H_0(ID_s, T_s, P_1)$.

2) Constructs the ciphertext $\sigma_1 = (\sigma, R_1')$ and sends it to receivers.

Designcryption: This algorithm runs by SM-IoT receivers of CLC system, with ciphertext σ_1 as input.

1) Compute $U_i' = R_1'(x_i + d_i)$, and $\gamma_i' = H_2(ID_s, ID_i, U_i', R_1')$.
2) Substitute γ_i' into $f(x)$, and figure out $f(\gamma_i') = x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \theta'$, and calculate $\rho' = H_3(\theta')$.
3) Decrypt $C' = Dec_{(\rho')}(S)$, and obtain $h' = H_5(ID_s, R_1', R_2, C', \theta', a_0, \ldots, a_{n-1})$. Then, checks if $h' = h$. If yes, continue to decrypt. Otherwise, output false symbol $\perp$ and aborts.
4) Computes $\alpha_i = H_4(\gamma_i', R_1')$, and then searches corresponding $H_4(\gamma_i, R_1)||c_i$ in C through α_i.
5) If there is no equation satisfies that $\alpha_i = H_4(\gamma_i, R_1)$ during the search process, aborts and returns $\perp$. Otherwise, recovers message $m_i' = c_i \oplus H_3(\gamma_i')$ and accept it.

V. CORRECTNESS PROOF AND SECURITY ANALYSIS

A. CORRECTNESS PROOFS

This is the correctness proof of our scheme.

Theorem 1: The verification of SM-IoT receiver's partial private key in Key Extraction Algorithm is correct.

Proof: Eqn. (5) $u_i P = T_i + h_i P_2 + H_1(ID_i, x_i P_2, T_i) P$ guarantees the correctness of the partial private key, because:

$$\begin{aligned} u_i P &= (t_i + h_i s_2 + H_1(ID_i, s_2 X_i, T_i)) P \\ &= t_i P + h_i s_2 P + H_1(ID_i, s_2 x_i P, T_i) P \\ &= T_i + h_i P_2 + H_1(ID_i, x_i P_2, T_i) P \end{aligned}$$

It can be seen from the above derivation process that the equation $u_i P = T_i + h_i P_2 + H_1(ID_i, x_i P_2, T_i) P$ holds, so it can be proved that our partial private key verification is correct.

Theorem 2: The computation of R_1' in *Designcryption Algorithm* is correct.

Proof: The derivation process of signature verification is guaranteed by the equation $h = h'$, and the correctness of

R_1' is required. R_1' is calculated as follow:

$$\begin{aligned} R_1' &= v(hR_2 + T_s + h_s P_1) \\ &= (hr_2 + d_s)^{-1} r_1 (hR_2 + T_s + h_s P_1) \\ &= r_1 (hr_2 + t_s + s_1 h_s)^{-1} (hr_2 + t_s + h_s s_1) P \\ &= r_1 P \\ &= R_1 \end{aligned}$$

R_1' can be verified in Theorem 4.

Theorem 3: $U_i' = R_1'(x_i + d_i)$ is equal to $U_i = r_1 h_i (PK_i + P_2)$, i.e., $U_i' = U_i$.

Proof:

$$\begin{aligned} U_i' &= R_1'(x_i + d_i) = r_1 P(x_i + d_i) \\ &= r_1 (x_i P + t_i P + h_i s_2 P) \\ &= r_1 (X_i + T_i + h_i P_2) \\ &= r_1 h_i (h_i^{-1}(X_i + T_i) + P_2) \\ &= r_1 h_i (PK_i + P_2) = U_i \end{aligned}$$

Theorem 4: The verification of $h = h'$ is correct by authorized receiver.

Proof: Receivers get the correct R_1', U_i' proved in *Theorem 2* and *Theorem 3*, and then get $\gamma_i' = \gamma_i$, and only the designated receivers can obtain correct $\rho' = \rho$. Then, the receiver uses ρ' to decrypt S to get correct C', and computes $h' = H_5(ID_s, R_1', R_2, C', \theta', a_0, \ldots, a_{n-1})$. It is obvious that the equation $h = h'$ holds, since $R_1' = R_1$ and $C' = C$.

B. SECURITY ANALYSIS

We analyze the security of this efficient signcryption scheme based on the security model defined in Section 3. The message confidentiality depends on the establishment of *Theorem 5* and *Theorem 6*, which follow *Game 1* and *Game 2* defined in Subsection D of Section 3 respectively. The unforgeability depends on the establishment of the *Theorem 7* which follows *Game 3*.

1) CONFIDENTIALITY

Theorem 5: The proposed scheme is IND-CCA2-I secure under the random oracle model, with the assumption that the CDHP is difficult.

Lemma 1: In the random oracle, if there is an adversary A_I wins the *Game 1* with non-negligible advantage ε, the CDHP can be solved by the challenger C, with non-negligible advantage $\varepsilon' \geq (1 - \frac{q_s(nq_s + q_{H_2})}{2^k})(1 - \frac{q_d}{2^k})$ within $\tau' \leq \tau + O(nq_s + q_{pk} + q_d)\tau_{pm}$, where τ_{pm} denotes the time to calculate a scalar point multiplication on ECC. The adversary A_I can make at least q_{H_i} times of H_i query, q_s times of signcryption query, q_d times of designcryption query, q_{sv} times of secret value query, q_{ppk} times of partial private key query, and q_{pk} times of public key query.

Proof: Assume that the adversary A_I attacks IND-CCA2-I security of the proposed scheme. With a tuple $\langle P, aP, bP \rangle$, C interacts with A_I and hopes to solve CDHP.

1) *Setup:* Challenger C sets $P_2 = aP$, and provides public parameter to adversary A_I. A_I chooses target identities $I = \{ID_i | i = 1, 2, \ldots, n\}$.

2) *Phase 1:* C keeps lists L_{H_i} of $H_i (i = 0, 1, \ldots, 5)$, and L_{PK} of keys.

a) $H_i (i = 0, 1, \ldots, 5)$ *query* (q_{H_i}): After receiving the H_i query, C checks if the corresponding tuple exists in the list L_{H_i}. If yes, challenger C retrieves and returns it to adversary A_I. Otherwise, challenger C randomly chooses an integer as result, returns to A_I, and stores in list L_{H_i}.

b) *Key-query:* If the tuple $\langle ID_j, x_j, d_j, PK_j \rangle$ exists in the L_{PK}, gets the tuple. Otherwise:

- If $ID_j \in I$, randomly chooses integer $x_j \in Z_p^*$, sets $d_j = \perp$, returns $SK_j = (x_j, \perp)$.
- If $ID_j \notin I$, randomly chooses integers $x_j, t_j, h_j \in Z_p^*$, sets $d_j = t_j + ah_j mod p$.

Then, sets $PK_j = h_j^{-1}(X_j + T_j)$, where $X_j = x_j P$, $T_j = t_j P$, updates h_j to L_{H_1}.

c) *Partial private key query* (q_{ppk}): With input ID_j, if $ID_j \in I$, C aborts. Otherwise, if ID_j exists in L_{PK}, returns d_j; if not, performs *Key-query* and returns d_j.

d) *Secret value query* (q_{sv}): If the input $ID_j \in I$, C returns $\perp$ and aborts. Otherwise, if exists in L_{PK}, C returns $SK_j = (x_j, d_j)$; if not, C performs *Key-query* and returns SK_j. If the public key of ID_j has been replaced, sets $d_j = \perp$.

e) *Public key query* (q_{pk}): Challenger C checks if the tuple of ID_j exists in L_{PK}. If yes, returns PK_j to the adversary A_I. Otherwise, performs *Key-query*, then returns PK_j and updates the key list L_{PK}.

f) *Replace public key* Replaces the public key of ID_j with PK_j', and sets $d_j = \perp$.

g) *Signcryption query* (q_s): The adversary A_I performs a signcryption query with ID_s, ID_j, and message M as inputs. Challenger C runs *Signcryption Algorithm* only if $ID_j \notin I$.

h) *Designcryption query* (q_d): A_I sends designcryption query with ID_s,ID_j, and ciphertext $\sigma = (S, R_2, v, h, A)$ as inputs. Challenger C checks if $ID_j \in I$. If yes, C aborts; otherwise, C runs the *Designcryption Algorithm* and returns the result.

3) *Challenge:* A_I submits two plaintexts M_0,M_1 ($M_\beta = \{m_i^\beta | i = 1, \ldots, n\}$) with equal length, and ID_s, ID_i ($i = 1, \ldots, n$) to the challenger C. C aborts if $ID_i \notin I$. Otherwise, C chooses a bit $\beta \in \{0, 1\}$, and computes $R_1 = bP$, $U_i = bh_i(PK_i + P_2)$, randomly chooses $\gamma_i^*, r_2^*, v^*, \theta^* \in Z_p^*$. Then, computes $R_2^* = r_2^* P$, and generates the ciphertext as $C_\beta = \{H_4(\gamma_i^*, R_1) || m_i^\beta \oplus H_3(\gamma_i^*) | i = 1, \ldots, n\}$. List equation $f(x) = \prod_{i=1}^{n}(x - \gamma_i^*) + \theta^* (\mathrm{mod} p)$ to calculate $A = \{a_i | i = 0, \ldots, n-1\}$. Computes $\rho^* = H_3(\theta^*)$, and $S_\beta = Enc_{\rho^*}(C_\beta)$, $h^* = H_5(ID_s, R_1, R_2^*, C_\beta, \theta^*, a_0, \ldots, a_{n-1})$. Finally, challenger C returns a ciphertext $\sigma^* = (S_\beta, R_2^*, v^*, h^*, A)$.

4) *Phase 2:* A_I performs a series of query as in *Phase 1*, except the query for the private key of target identities whose public key has been replaced, the partial private key of target identities, or the designcryption query for σ^*.

5) *Guess:* The adversary A_I outputs a bit β' according to the phases performed above. If $\beta' = \beta$, then A_I wins this game, and the challenger outputs $abP = U_i h_i^{-1} - R_1$ as the solution to CDHP. Otherwise, C aborts and outputs $\perp$.

From the discussion above, the conclusion that the advantage of the challenger C sovling the CDHP is analyzed as follow. The probability of adversary A_I failing in signcryption query is $\frac{q_s(nq_s+q_{H_2})}{2^k}$, and the probability of C rejecting a valid ciphertext during designcryption query is $\frac{q_d}{2^k}$. Therefore, the total advantage of challenger C to solve CDHP is $\varepsilon' \geq (1-\frac{q_s(nq_s+q_{H_2})}{2^k})(1-\frac{q_d}{2^k})$, within $\tau' \leq \tau + O(nq_s+q_{pk}+q_d)\tau_{pm}$.

Theorem 6: The proposed scheme is IND-CCA2-II secure with the assumption that the CDHP is difficult.

Lemma 2: If the adversary A_{II} wins the *Game 2* with non-negligible advantage ε, (A_{II} can query at most q_{sv} times of secret value, q_{ppk} times of partial private key, q_{H_i} times of H_i query, q_s times of signcryption query, and q_d times of designcryption query), the CDHP can be solved by the simulator C, with non-negligible advantage $\varepsilon' \geq \varepsilon - \frac{q_{H_2} q_d}{2^k}$.

Proof: Assume that the adversary A_{II} attacks IND-CCA2-II security of the scheme.

1)*Setup:* Challenger C sets $P_2 = s_2 P$, sends system public parameter to A_{II}. Adversary A_{II} chooses target identities $I = \{ID_i | i = 1, 2, \ldots, n\}$.

2) *Phase 1:* Challenger C keeps the lists L_{H_i} of H_i query results and L_{PK} of key query results. A_{II} makes polynomial bounded number of query as follow.

a) H_i *($i = 0, 1, \ldots, 5$) query (q_{H_i}):* Challenger C responds as in *Phase 1* of *Game 1*.

b) *Key query:* With ID_j as input, C checks if exists in L_{PK}. If yes, C retrieves the result. Otherwise:

- If $ID_j \in I$, sets $x_j = \perp$.
- If $ID_j \notin I$, randomly chooses $t_j, h_j \in Z_p^*$, sets $x_j = a$.

Then, sets $SK_j = (x_j, d_j)$, computes $d_j = t_j + s_2 h_j \bmod p$, $PK_j = h_j^{-1}(T_j + X_j)$, where $T_j = t_j P$, $X_j = x_j P$.

c) *Public key query (q_{pk}):* Upon receiving ID_j, challenger C checks if the corresponding tuple exists in L_{PK}, and retrieves public key and returns back if yes. Otherwise C makes a key query to obtain the corresponding public key.

d) *Secret value query (q_{sv}):* Upon receiving ID_j, challenger C checks if $ID_j \in I$. If yes, then returns $\perp$ and aborts. If not, C retrieves the result x_j from L_{PK}, or performs key query to obtain x_j, and then returns it to the adversary A_{II}.

e) *Partial private key query (q_{ppk}):* If the tuple of ID_j exists in list L_{PK}, challenger$C$ retrieves the corresponding partial private key from L_{PK}. Otherwise, c performs key query to get the answer.

f) *Signcryption query (q_s):* With ID_s, $ID_j (ID_j \notin I)$, and message M as inputs, challenger C runs *Signcryption Algorithm* to generate corresponding signcryption ciphertext σ.

g) *Designcryption query (q_d):* Adversary A_{II} performs the designcryption query with ID_s, $ID_j (ID_j \notin I)$, and cipher-text σ as inputs. The challenger C runs the *Designcryption Algorithm* to obtain the plaintext, and then returns the result.

3) *Challenge:* The adversary A_{II} submits two plaintexts M_0, M_1 ($M_\beta = \{m_i^\beta | i = 1, \ldots, n\}$) with equal length, and ID_s, ID_i to C. The challenger C aborts if $ID_i \notin I$. Otherwise, C chooses a bit $\beta \in \{0, 1\}$, computes $R_1 = bT_i$, $U_i = b(X_i + T_i)$, chooses $\gamma_i^*, r_2^*, v^*, \theta^* \in Z_p^*$, and computes $R_2^* = r_2^* P$, h^* and $A = \{a_i | i = 0, \ldots, n-1\}$. Then, challenger generates the ciphertext as C_β, $\rho^* = H_3(\theta^*)$, and $S_\beta = Enc_{\rho^*}(C_\beta)$. Finally, C returns a signcryption ciphertext $\sigma^* = (S_\beta, R_2^*, v^*, h^*, A)$.

4) *Phase 2:* The adversary A_{II} performs queries as in *Phase 1*, except secret key query of any target identity, private key query of receivers whose public key has been replaced and the designcryption query of target signcryption ciphertext σ^*.

5) *Guess:* A_{II} outputs a bit β' according to the phases performed above. If $\beta' = \beta$, then A_{II} wins the game, and the challenger outputs $abP = U_i - R_1$ as the solution to CDHP. Otherwise, challenger C outputs $\perp$ and aborts.

Through the interaction with A_{II}, the probability advantage of challenger C breaking CDHP within $\tau' \leq \tau + O(nq_s + q_{pk} + q_d)\tau_{pm}$ is $\varepsilon' \geq \varepsilon(1 - \frac{q_s(nq_s+q_{H_2})}{2^k})(1 - \frac{q_d}{2^k})$.

2) UNFORGEABILITY

Theorem 7: The proposed scheme is EUF-CMA secure with the assumption that the ECDLP is difficult.

Lemma 3: If the forger F wins the *Game 3* with non-negligible advantage ε, the ECDLP can be solved by the challenger C, with non-negligible advantage ε'.

Proof: C looks forward to solving this answer through the interaction with forger F.

1) *Setup:* C runs the algorithm to generate system public parameter, sets $P_1 = s_1 P$ and sends *param* and KGC's master key s_2 to F. F chooses a target identity ID_s'.

2) *Attack:* Forger F performs a series of queries as follow.

a) H_i *query (q_{H_i}):* Upon receiving the query on identity ID_s, C checks if the corresponding tuple result exists in L_{H_i}. If yes, returns the result. If not, randomly chooses an integer, then returns it back to the forgery, and stores in the list L_{H_i}.

b) *Private key query (q_{sk}):* The forger F submits ID_s to C. Then, challenger C checks if $ID_s = ID_s'$. If yes, C returns $\perp$ and aborts. Otherwise:

- If ID_s corresponding tuple exists in L_{SK}, then retrieve and returns the result.
- If not, C sets $SK_s = t_s + s_1 h_s$, $T_s = t_s P$, where $t_s \in Z_p^*$. Then returns back, and stores the tuple.

TABLE 2. Comparison of functions.

Schemes	Heterogenous	No Certificate Management Burden	Pairing Free	Multi -Message	Multi -Receiver	Wireless Secure Channel Requirements
Sun et al. [51]	Yes	No	No	No	Yes	Yes
Huang et al. [52]	Yes	Yes	No	No	Yes	Yes
Islam et al. [45]	No	Yes	Yes	No	Yes	Yes
Hung et al. [44]	No	Yes	No	No	Yes	Yes
Li et al. [39]	No	Yes	No	No	No	Yes
He et al. [58]	No	Yes	Yes	No	Yes	Yes
Niu et al. [55]	Yes	Yes	No	Yes	Yes	Yes
Wang et al. [59]	Yes	No	No	Yes	Yes	Yes
Karati et al. [27]	No	Yes	No	No	No	Yes
Pang et al.-I [46]	No	Yes	Yes	No	No	Yes
Pang et al.-II [50]	No	Yes	Yes	Yes	Yes	Yes
Ours	Yes	Yes	Yes	Yes	Yes	No

c) *Signcryption query (q_s):* The forger F submits a signcryption query with ID_s,ID_i, and n messages m_i, $i = 1, 2, \ldots, n$ as inputs. If $ID_s \neq ID'_s$, C runs the *Signcryption Algorithm* as normal, then returns the signcryption ciphertext σ to F. Note that the hash values used in *Signcryption Algorithm* are retrieved from corresponding L_{H_i} hash oracles.

3) *Forgery:* If F is an efficient forger, then by forking lemma [60], F' can forge two signcryption ciphertext $\sigma' = (S', R'_2, v', h', A'), \sigma^* = (S', R^*_2, v^*, h^*, A^*)$. We can combine the two equations, $R'_1 = v'(d'_sP+h'R'_2), R^*_1 = v^*(d'_sP+h^*R'_2)$. Then, the algorithm outputs $a = \frac{(h^*-h')r'_2}{v'-v^*}$.

Thus the ECDLP can be solved within time $\tau' \leq 120686q_s\tau/\varepsilon$, and the advantage of F forges a signature in time τ is $\varepsilon \geq 10(q_s + 1)(q_s + q_{H_5})/2^k$, the derivations is similar to Barreto *et al.* [56].

VI. PERFORMANCE ANALYSIS AND FUNCTIONAL COMPARISON

This section illustrates the advantages of the proposed scheme through making a comparison of functions and computational efficiency between the proposed scheme and the existing ones [27], [39]– [52], [44]– [55], [58], [59], because these schemes have similar functions as ours. We implement a series of tests of [44], [50], [55], [58], as well as corresponding figure, which is intended to show the performance comparison results more intuitively.

A. COMPARISON OF FUNCTIONS

We compare functions of our scheme and schemes [27], [39]– [52], [44]– [55], [58], [59]. The results is shown in Table 2. There are four schemes [51], [52], [55], [59] consider the heterogeneity of SM-IoT. However, [51], [52], [59] have the burden of certificate management, because they are constructed based on PKI. Therefore, they are not suitable for the SM-IoT. Reference [39] takes the public verifiability into consideration, which shifts most computational cost of designcrypt from the SM-IoT receiver to the gateway. But this scheme not consider the heterogeneity, which limits its application in the SM-IoT environment.

Multi-receiver and multi-message scheme are satisfied by schemes [44], [50], [55], [59], and there are four schemes [45], [51], [52], [58] only meet multi-receiver function. However, as we can see, schemes [27], [39]– [52], [44], [55], [59] are constructed based on bilinear pairing, which is an expensive operation for the SM-IoT environment.

Through hiding the SM-IoT receiver's partial private key of CLC system during key generation phase, our scheme no longer need wireless secure channel to transmit partial private key. Therefore, our scheme is more suitable for wireless SM-IoT environment.

Through the comparison and analysis above, it is obvious that compared with these schemes, our scheme meets all the functions mentioned in Table 2, including heterogeneity, multi-message and multi-receiver, pairing free, and no requirement for wireless secure channel. The proposed scheme transmits part of computational overhead to the gateway through outsourcing, meets the heterogeneity feature of the SM-IoT by constructing the scheme based on IBC and CLC, and improves the efficiency of encryption and decryption by using scalar point multiplication on ECC instead of bilinear pairing. Therefore, our scheme has higher efficiency, and is more practical for application in the SM-IoT environment.

B. COMPARISON AND ANALYSIS OF PERFORMANCE

In this subsection, to have better understanding the Table 3, we define notations to denote computational complexity of different mathematical operations, and give the descriptions of their definition in Table 2. In order to provide a numerical result, we use C and Pairing-Based Cryptography (PBC) Library [61] to implement related mathematical operations. The well-known super-singular elliptic curve type-A $y^2 = x^3 + x$ is used to reach the same security level as 1024-bit RSA, the curve group has 160-bit group order, 512-big field size, and the embedding degree of the curve is 2. Our implementation runs on a Personal Computer with intel(R) Core(TM) i3-3220 CPU @ 3.3GHz, VMware 15.0.4, Linux ubuntu 18.04 operating system with 3 GB of RAM. The execution time is computed considering the average of ten succeeding run with different inputs. Table 2 displays the

TABLE 3. Notations and benchmark.

Symbol	Definition	Execution time in s
T_p	It refers to bilinear pairing operation's calculation time.	0.001289
T_e	It refers to modular exponentiation operation's calculation time.	0.001613
T_{ee}	It refers to pairing-based exponentiation operation's calculation time.	0.000164
T_{pm}	It refers to the calculation time of scalar point multiplication on ECC operation.	0.000137
T_h	It refers to Map-to-Point hash function operation's calculation time.	0.003168
T_{pa}	It refers to the calculation time of point addition on ECC operation.	0.000011

TABLE 4. Comparison of computational complexity.

Schemes	Encryption/Signcryption	Decryption/Designcryption	
		FN/Gateway	Receiver
Sun et al. [51]	$nT_p + nT_{ee} + 2nT_{pm}$	-	$2T_p + T_{ee}$
Huang et al. [52]	$2T_{pm} + nT_h + nT_p$	-	T_p
Islam et al. [45]	$(2n+1)T_{pm} + 2nT_{pa}$	-	T_{pm}
Hung et al. [44]	$nT_p + nT_{ee} + nT_h + (n+1)T_{pm}$	-	$T_{pm} + T_p$
Li et al. [39](*)	$3nT_{ee}$	$3nT_{ee} + nT_{pm} + nT_p$	T_{ee}
He et al. [58]	$(3n+1)T_{pm} + nT_{pa}$	-	$2T_{pm}$
Niu et al. [55]	$(n+2)T_{pm} + 2nT_p + 2nT_{ee}$	-	$4T_p + T_{pm} + T_{pa}$
Wang et al.-IBC-PKI [59]	$(n+1)T_{ee} + nT_{pm}$	-	$2T_p + 2T_{pm} + T_{ee}$
Karati et al. [27](*)	$4nT_{ee}$	-	$2T_p + 2T_{ee}$
Pang et al.-I [46](*)	$(n+1)T_{pm} + nT_{pa}$	-	$3T_{pm} + 2T_{pa}$
Pang et al.-II [50]	$(n+1)T_{pm} + nT_{pa}$	-	$3T_{pm} + T_{pa}$
Ours	$(n+2)T_{pm} + nT_{pa}$	$3T_{pm} + 2T_{pa}$	T_{pm}

(*) indicates that the scheme did not meet the requirements of both multi-message and multi-receiver signcryption scheme; n indicates the number of receivers.

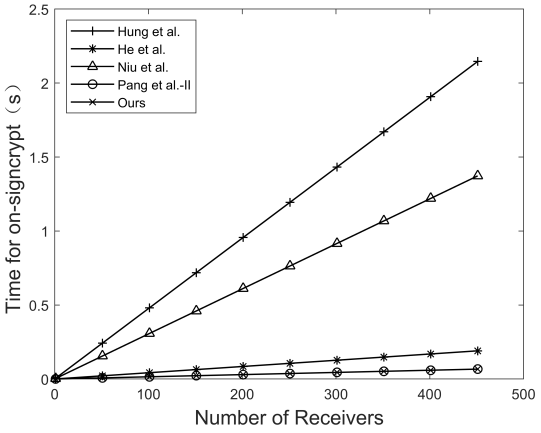

FIGURE 2. The computational time of *Signcryption Algorithm*.

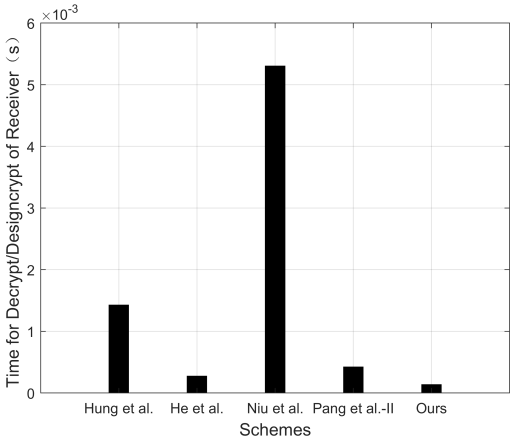

FIGURE 3. Receivers' computational time of *Decryption/Designcryption*.

execution time of different mathematical operations used in the schemes discussed. It is important to note that we only consider expensive operations. We analysis the computational complexity of schemes [44], [50], [55], [58], and our scheme. The comparison results are shown in Table 4.

For *Signcryption Algorithm*, e.g., Sun and Li [51] needs n bilinear pairing operations, $2n$ point multiplications, and n exponentiation after pairing, Islam *et al.* [45] requires $(2n+1)$ point multiplications and $2n$ additions on ECC, Niu *et al.* [55] needs $(n+2)$ point multiplications, $2n$ bilinear pairing operations and $2n$ exponentiation after pairing, whereas our scheme only needs $(n+2)$ point multiplication and n addition on ECC, which is lower than most schemes listed in TABLE 4, and is about the same as the schemes [46], [50]. Nevertheless, for *Designcryption/decryption Algorithm*, the SM-IoT receiver in our scheme only requires one point multiplication on ECC, which is lower than schemes [46], [50]. As can be seen from the TABLE 4, the efficiency of our scheme is relatively improved in both sender and receiver sides.

To show the results intuitively, we present the execution time of *Signcryption Algorithm* of schemes [44], [50], [55], [58] in Fig. 2, and the execution time of *Designcryption/decryption Algorithm* at SM-IoT receiver side in Fig. 3, which are based on the execution time implemented with Pairing-Based Cryptography (PBC) Library. From the Fig. 2, we can see that the signcryption computational time of our scheme is the same as the scheme proposed by Pang *et al.* [50], which is more efficient than other compared schemes. The Fig. 3 shows that our scheme has the lowest calculation time in the receiver side. In the light of Table 4, Fig. 2, and Fig. 3, we can draw the conclusion that our scheme has less calculation time in both sender and receiver sides.

VII. CONCLUSION

In this paper, we have proposed a signcryption scheme for SM-IoT, to achieve secure and efficient multi-message and multi-receiver communication from senders of IBC system to receivers of CLC system. We hide the partial private key during the key generation phase of the traditional CLC system, which means SM-IoT receivers and the KGC no longer need wireless secure channel to transmit their partial private keys. The proposed scheme is constructed based on ECC which has higher efficiency, and do not employ bilinear pairing and exponentiation operations. Besides, our scheme outsourced part of computational overhead to the gateway, so as to minimize the computation costs of the SM-IoT receivers. And the designated receivers can verify signature and outsourced result securely. Therefore, on the whole, our scheme has less computational complexity and higher efficiency compared with the schemes proposed before in both sender side and receiver side. Therefore, it is more suitable for the heterogeneous SM-IoT environment. For further research in our work, we will consider aggregate signcryption schemes between IBC and CLC, to achieve efficient mutual multi-communication in the heterogeneous SM-IoT.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] N. E. Petroulakis, E. Lakka, E. Sakic, V. Kulkarni, K. Fysarakis, I. Somarakis, J. Serra, L. Sanabria-Russo, D. Pau, M. Falchetto, D. Presenza, T. Marktscheffel, K. Ramantas, P.-V. Mekikis, L. Ciechomski, and K. Waledzik, "SEMIoTICS architectural framework: End-to-end security, connectivity and interoperability for industrial IoT," in *Proc. Global IoT Summit (GIoTS)*, Aarhus, Denmark, Jun. 2019, pp. 1–6.

[3] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4265–4276, Aug. 2015.

[4] K. Fan, W. Jiang, Q. Luo, H. Li, and Y. Yang, "Cloud-based RFID mutual authentication scheme for efficient privacy preserving in IoV," *J. Franklin Inst.*, to be published.

[5] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A lightweight authentication scheme for cloud-based RFID healthcare systems," *IEEE Netw.*, vol. 33, no. 2, pp. 44–49, Mar. 2019.

[6] K. Fan, Q. Luo, K. Zhang, and Y. Yang, "Cloud-based lightweight secure RFID mutual authentication protocol in IoT," *Inf. Sci.*, to be published.

[7] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, "Efficient and privacy preserving access control scheme for fog-enabled IoT," *Future Gener. Comput. Syst.*, vol. 99, pp. 134–142, 2019.

[8] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, and Y. Xiang, "Data-driven cyber security in perspective–intelligent traffic analysis," *IEEE Trans. Cybern.*, to be published.

[9] N. Sun, J. Zhang, P. Rimba, S. Gao, Y. Xiang, and L. Y. Zhang, "Data-driven cybersecurity incident prediction: A survey," *IEEE Commun. Surveys Tutr.*, vol. 21, no. 2, pp. 1744–1772, 2nd Quart., 2018.

[10] J. Zhang, Y. Xiang, Y. Wang, W. Zhou, Y. Xiang, and Y. Guan, "Network traffic classification using correlation information," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 104–117, Jan. 2013.

[11] X. Chen, C. Li, D. Wang, S. Wen, J. Zhang, S. Nepal, Y. Xiang, and K. Ren, "Android HIV: A study of repackaging malware for evading machine-learning detection," *IEEE Trans. Inf. Forensics Security*, vol. 15, no. 1, pp. 987–1001, Jul. 2019.

[12] L. Liu, O. de Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," *IEEE Commun. Surveys Tutr.*, vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.

[13] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of Things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[14] V. Sharma, "Security, privacy and trust for smart mobile-Internet of things (M-IoT): A survey," 2019, *arXiv:1903.05362*. [Online]. Available: https://arxiv.org/abs/1903.05362

[15] J. Camhi, "Former Cisco CEO John Chambers predicts 500 billion connected devices by 2025," Business Insider, New York, NY, USA, 2015.

[16] N. Zhang, R. Wu, S. Yuan, C. Yuan, and D. Chen, "RAV: Relay aided vectorized secure transmission in physical layer security for Internet of things under active attacks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8496–8506, Oct. 2019.

[17] K. Fan, S. Sun, Z. Yan, Q. Pan, H. Li, and Y. Yang, "A blockchain-based clock synchronization scheme in IoT," *Future Generation Comput. Syst.*, vol. 101, pp. 524–533, 2019.

[18] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption)," in *Proc. Annu. Int. Cryptol. Conf.* (Lecture Notes in Computer Science), vol. 1294. Berlin, Germany: Springer, 1997, pp. 165–179.

[19] T. Matsuda, K. Matsuura, and J. C. N. Schuldt, "Efficient constructions of signcryption schemes and signcryption composability," in *Proc. Int. Conf. Cryptol. India* (Lecture Notes in Computer Science), vol. 5922. Springer, 2009, pp. 321–342.

[20] J. H. An, "Authenticated encryption in the public-key setting: Security notions and analyses," IACR Cryptol. ePrint Arch., Tech. Rep., 2001.

[21] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* (Lecture Notes in Computer Science), vol. 196. Berlin, Germany: Springer, 1984, pp. 47–53.

[22] J. Malone-Lee, "Identity-based signcryption," IACR Cryptol. ePrint Arch., Tech. Rep., no. 98, Jun. 2002, [Online]. Available: http://eprint.iacr.org/2002/098

[23] B. Libert and J. J. Quisquater, "A new identity based signcryption scheme from pairings," in *Proc. IEEE Inf. Theory Workshop*, Paris, France, Mar./Apr. 2003, pp. 155–158.

[24] S. S. M. Chow, S.-M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Proc. Int. Conf. Inf. Secur. Cryptol.* (Lecture Notes in Computer Science), vol. 2971. Berlin, Germany: Springer, 2003, pp. 352–369.

[25] X. Boyen, "Multipurpose identity-based signcryption," in *Proc. Annu. Int. Cryptol. Conf.* (Lecture Notes in Computer Science), vol. 2729. Berlin, Germany: Springer, 2003, pp. 383–399.

[26] F. Li and M. K. Khan, "A survey of identity-based signcryption," *IETE Tech. Rev.*, vol. 28, no. 3, pp. 265–272, 2011.

[27] A. Karati, S. H. Islam, G. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2904–2914, Aug. 2018.

[28] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2894. Berlin, Germany: Springer, 2003, pp. 452–473.

[29] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proc. ACM Symp. Inf., Comput. Commun. Secur.*, Tokyo, Japan, 2008, pp. 369–372.

[30] C. Wu and Z. Chen, "A new efficient certificateless signcryption scheme," in *Proc. Int. Symp. Inf. Sci. Eng.*, vol. 1, Dec. 2008, pp. 661–664.

[31] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "On the security of certificateless signcryption schemes," Cryptol. ePrint Arch., Tech. Rep., 2009.

[32] Z. Liu, Y. Hu, X. Zhang, and H. Ma, "Certificateless signcryption scheme in the standard model," *Inf. Sci.*, vol. 180, no. 3, pp. 452–464, 2010.

[33] W. Xie and Z. Zhang, "Efficient and provably secure certificateless signcryption from bilinear maps," in *Proc. IEEE Int. Conf. Wireless Commun., Netw. Inf. Secur.*, Jun. 2010, pp. 558–562.

[34] S. S. D. Selvi, S. S. Vivek, and C. P. Rangan, "Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Springer, 2009, pp. 75–92.

[35] W. Xie and Z. Zhang, "Certificateless signcryption without pairing," IACR Cryptol. ePrint Arch., Tech. Rep., 2010, p. 187.

[36] X. Jing, "Provably secure certificateless signcryption scheme without pairing," in *Proc. Int. Conf. Electron. Mech. Eng. Inf. Technol.*, vol. 9, Aug. 2011, pp. 4753–4756.

[37] Y. Zhou, B. Yang, and W. Zhang, "Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing," *Discrete Appl. Math.*, vol. 204, pp. 185–202, 2016.

[38] F. Li, Y. Han, and C. Jin, "Certificateless online/offline signcryption for the Internet of things," *Wireless Netw.*, vol. 23, no. 1, pp. 145–158, 2017.
[39] F. Li, J. Hong, and A. A. Omala, "Efficient certificateless access control for industrial Internet of things," *Future Gener. Comput. Syst.*, vol. 76, pp. 285–292, 2017.
[40] W. Shi, N. Kumar, P. Gong, N. Chilamkurti, and H. Chang, "On the security of a certificateless online/offline signcryption for Internet of things," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 5, pp. 881–885, 2015.
[41] S. Duan and Z. Cao, "Efficient and provably secure multi-receiver identity-based signcryption," in *Proc. Australas. Conf. Inf. Secur. Privacy* (Lecture Notes in Computer Science), vol. 4058. Berlin, Germany: Springer, 2006, pp. 195–206.
[42] H.-Y. Chien, "Improved anonymous multi-receiver identity-based encryption," *Comput. J.*, vol. 55, no. 4, pp. 439–446, 2011.
[43] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Trans. Comput.*, vol. 59, no. 9, pp. 1239–1249, Sep. 2010.
[44] Y.-H. Hung, S.-S. Huang, Y.-M. Tseng, and T.-T. Tsai, "Efficient anonymous multireceiver certificateless encryption," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2602–2613, Dec. 2017.
[45] S. H. Islam, M. K. Khan, and A. M. Al-Khouri, "Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing," *Secur. Commun. Netw.*, vol. 8, no. 13, pp. 2214–2231, Sep. 2015.
[46] L. Pang, M. Kou, M. Wei, and H. Li, "Efficient anonymous certificateless multi-receiver signcryption scheme without bilinear pairings," *IEEE Access*, vol. 6, pp. 78123–78135, 2018.
[47] M. Seo and K. Kim, "Electronic funds transfer protocol using domain-verifiable signcryption scheme," in *Proc. Int. Conf. Inf. Secur. Cryptol.* (Lecture Notes in Computer Science), vol. 1787. Berlin, Germany: Springer, 1999, pp. 269–277.
[48] H. M. Elkamchouchi and E. A. A. Hagras, "An efficient Public Key Multi-Messages Multi-Recipients Elliptic Curve Signcryption (PK-MM-ECS) scheme," in *Proc. Nat. Radio Sci. Conf.*, Tanta, Egypt, Mar. 2008, pp. 1–10.
[49] A. Kumar and M. M. Ansari, "Multi message signcryption based on chaos with public verifiability," *Int. J. Sci. Technol. Res.*, vol. 2, no. 5, pp. 194–198, May 2013.
[50] L. Pang, M. Wei, and H. Li, "Efficient and anonymous certificateless multi-message and multi-receiver signcryption scheme based on ECC," *IEEE Access*, vol. 7, pp. 24511–24526, 2019.
[51] Y. X. Sun and H. Li, "Efficient signcryption between TPKC and IDPKC and its multi-receiver construction," *Sci. China*, vol. 53, no. 3, pp. 557–566, 2010.
[52] Q. Huang, D. S. Wong, and G. Yang, "Heterogeneous signcryption with key privacy," *Comput. J.*, vol. 54, no. 4, pp. 525–536, 2011.
[53] Y. Zhang, L. Zhang, Y. Zhang, H. Wang, and C. Wang, "Clpkc-to-tpki heterogeneous signcryption scheme with anonymity," *Acta Electron. Sinica*, vol. 44, no. 10, pp. 2432–2439, 2016.
[54] Y. Li, C. Wang, Y. Zhang, and S. Niu, "Privacy-preserving multi-receiver signcryption scheme for heterogeneous systems," *Secur. Commu. Netw.*, vol. 9, no. 17, pp. 4574–4584, 2016.
[55] S. Niu, L. Niu, X. Yang, C. Wang, and X. Jia, "Heterogeneous hybrid signcryption for multi-message and multi-receiver," *PloS one*, vol. 12, no. 9, 2017.
[56] P. S. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3788. Berlin, Germany: Springer, 2005, pp. 515–532.
[57] P.-Y. Ting, J.-L. Tsai, and T.-S. Wu, "Signcryption method suitable for low-power IoT devices in a wireless sensor network," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2385–2394, Sep. 2018.
[58] D. He, H. Wang, L. Wang, J. Shen, and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Comput.*, vol. 21, no. 22, pp. 6801–6810, Nov. 2017.
[59] C. Wang, C. Liu, Y. Li, H. Qiao, and L. Chen, "Multi-message and multi-receiver heterogeneous signcryption scheme for ad-hoc networks," *Inf. Secur. J., Global Perspective*, vol. 26, no. 3, pp. 136–152, 2017.
[60] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.
[61] *The Pairing-Based Cryptography Library*, [Online]. Available: https://crypto.stanford.edu/pbc/

JIANYING QIU was born in Hunan, China, in 1995. She received the B.S. degree in information security from Chongqing University, in 2018. She is currently pursuing the master's degree with the State Key Laboratory of Integrated Service Networks, Xidian University. Her research interests are the IoT security and information security.

KAI FAN received the B.S. degree in telecommunication engineering, the M.S. degree in cryptography and telecommunication, and the Ph.D. degree in information system from Xidian University, China, in 2002, 2005, and 2007, respectively. He is currently a Professor with the State Key Laboratory of Integrated Service Networks, Xidian University. He has published over 70 articles in journals and conferences. He holds nine Chinese patents. He has managed five national research projects. His research interests include the IoT security and information security.

KUAN ZHANG received the B.S. degree in communication engineering and the M.S. degree in computer applied technology from Northeastern University, China, in 2009 and 2011, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2016. He was a Postdoctoral Fellow with the University of Waterloo, from 2016 to 2017. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, USA. He has published over 50 articles in journals and conferences. His research interests include cyber security, big data, and cloud/edge computing. He was a recipient of the Best Paper Award at the IEEE WCNC 2013 and the Securecomm 2016.

QIANG PAN received the B.S. degree in electronic information science and technology from Xidian University, Xi'an, China, in 2017, where he is currently pursuing the master's degree with the State Key Laboratory of Integrated Service Networks. His research interests are cloud security, the IoT security, and network and information security.

HUI LI was born in Shaanxi, China, in 1968. He received the B.S. degree in radio electronics from Fudan University, in 1990, and the M.S. and Ph.D. degrees in telecommunications and information system from Xidian University, in 1993 and 1998, respectively. He is currently a Professor with Xidian University. His research interest includes network and information security.

YINTANG YANG was born in Hebei, China, in 1962. He received the Ph.D. degree in semiconductor from Xidian University, Xi'an, China. He is currently a Professor with the Key Laboratory of the Ministry of Education for Wide Band-Gap Semiconductor Materials and Devices, Xidian University. His research interests include semiconductor materials and devices, and network and information security.